(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 June 2001 (07.06.2001)

PCT

(10) International Publication Number
WO 01/40908 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/EP00/11790

(22) International Filing Date:
24 November 2000 (24.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9928208.9 29 November 1999 (29.11.1999) GB

(71) Applicant *(for all designated States except US)*: **MEDICAL DATA SERVICES GMBH** [DE/DE]; An der Alten Ziegelei 20, 48157 Munster (DE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **ELFERING, Ingo** [DE/US]; SmithKline Beecham, 709 Swedeland Road, King of Prussia, PA 19406 (US). **RESCHKE, Julian** [DE/DE]; Medical Data Services GmbH, An der Alten Ziegelei 20, 48157 Munster (DE).

(74) Agent: **GIDDINGS, Peter, John**; SmithKline Beecham, Corporate Intellectual Property, Two New Horizons Court, Brentford, Middlesex TW8 9EP (GB).

(81) Designated State *(national)*: US.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/40908 A2

(54) Title: SECURE CONTENT EMBEDDING

(57) Abstract: The present invention relates to systems, methods and computer program products for embedding sensitive data in a secure fashion in an otherwise unsecure document on a computer.

Secure Content Embedding

Area of the Invention

The present invention relates to computer-based secure display of sensitive content from one data source in a second, potentially unsecure document. In particular, the present invention relates to systems, methods and computer program products for embedding sensitive data in a secure fashion in an otherwise unsecure document on a computer.

The present invention finds particular, but not exclusive, application to the healthcare industry. It can be used in any application where sensitive or confidential data in a source file is to be made available through second access provider where the second access provider may not be secure. Internet-based systems in particular benefit from the application of this invention.

As an example, a problem encountered in healthcare systems is that medical information needs to be easily accessible to a patient. Notifications about lab results, prescription renewals, etc. can both reduce cost in health care and increase health of a person when delivered in a timely manner. By way of example of the challenge, a possible way of providing this information would be that of placing on the front page of a newspaper which the patient is known to read every day. This would however violate patient privacy concerns since the same newspaper may be delivered to millions of other persons as well. One solution, in this newspaper example, would be to print a personalized version of the newspaper which would only be delivered to that person. This is what portal sites like Netscape, Yahoo and America OnLine on the Internet excel at. They deliver an up-to-the-minute, personal version of a newspaper digitally on a person's computer. However in order to place personal medical information on these pages, a content provider would have to transmit this information to the portal site first. The portal site would embed this into their page and transmit the page to the user. This is basically how Netscape's "Rich Site Summary" works.

The present invention describes a method of embedding information into a portal page without having to give the data to the portal. The data is securely transmitted between the patient and the medical content provider. No information is disclosed to a third party.

Summary of the Invention

In a first aspect this invention relates to a method for creating secure access to data in a first secure file by way of an insecure portal in a distributed computing environment, the process comprising:

accessing an insecure portal provider by a requestor using a browser,

creating, by the requestor, a document unique to the requestor on that insecure portal,

embedding, by said portal in said document, a reference to a java applet which can open a connection to the first secure file,

causing the requestor's browser, while loading the insecure document, to see the java applet and request it from the secure file,

transferring the requested java applet to the requestor's browser which starts it, thereby opening a connection to the secure file,

causing the secure file to generate code which is transmitted to the requestor's browser,

causing the applet on the requestor's browser to receive said code and insert it into the portal's document.

In a second aspect, this invention provides a means for accessing a secure file through an insecure portal on a distributed computing system, the process comprising:

activating a java applet embedded in the insecure portal document wherein the java applet which provides secure access to the secure file, wherein the embedded applet is created by:

accessing an insecure portal provider by a requestor using a browser,

creating, by the requestor, a document unique to the requestor on that insecure portal,

embedding, by said portal in said document, a reference to a java applet which can open a connection to the first secure file,

causing the requestor's browser, while loading the insecure document, to see the java applet and request it from the secure file,

transferring the requested java applet to the requestor's browser which starts it, thereby opening a connection to the secure file,

causing the secure file to generate code which is transmitted to the requestor's browser,

causing the applet on the requestor's browser to receive said code and insert it into the portal's document.

Description of the Figures

Figure 1 is a block diagram of content embedding in a web portal.

Figure 2 is a block diagram of content embedding with license

Description of the Invention

The present invention uses facilities in HTML, Java and Javascript to enable the content delivery. The present invention does not require any special software to be installed on the user's machine other than a HTML browser like Internet Explorer or Netscape Communicator. It can be run on any personal computer and server. In the description the fictitious names are used for better readability:

- User – Susan
- Portal – www.portal.com, knows Susan as "John Doe"
- Content Provider – www.medrec.com, knows Susan as "User1772"

The scenario is started by Susan's logging on to the portal and asking it to generate a personal web page for her. The portal has ways and means to determine that the request comes from a "John Doe" source, which is how it characterizes Susan's request. Prior to logging on to the personal web page generating portal, Susan has configured another portal to show her information from www.medrec.com. The portal generates "John Doe's" page and leaves space for the content from "www.medrec.com", a medical records provider on the web. In this space, the portal includes a reference to a java applet of "www.medrec.com".

Susan's browser, while loading the HTML page, sees the reference to the java applet and requests it from www.medrec.com. The applet is transferred and Susan's browser starts it. The applet opens a connection to www.medrec.com. Medrec uses a method (described below) to determine that the request came on behalf of "User1772". medrec generates a piece of HTML code fragment, which is to be displayed on the browser. The applet receives the HTML code fragment and inserts it into the portal's page. Now Susan's browser shows a page where the information from www.medrec.com is listed integrated among the other news from www.portal.com. Details of the implementation of this are provided. A sequence diagram is given in Figure 1.

It is not relevant to the present invention how the portal learns that Susan's request is for "John Doe". However the content provider needs a way to identify that information is to be generated for User1772 – the identity under which Susan is known to the content provider.

The easiest method is to use the HTML cookie scheme. Susan is required to login once to www.medrec.com for "User1772" with her password. Medrec then stores a cookie in Susan's browser. This cookie is later transmitted with the applets request and allows

medrec to generate information for User1772. The cookie scheme does not provide optimal security. Several browser's default configuration allow foreign sites to read Medrec's cookie. Thus, other sites can "steal" the cookie and use them for their own request. This would give such a site access to Susan's information. The stolen cookie can carry a timestamp, so that it expires after a certain time. Assuming this time to be 7 days, this would require Susan to login at least every week to www.medrec.com. The advantage is that a stolen cookie could only be used in this time window. This is an improved security. A preferred security scheme is described below. Note however, that the basic scheme is of interest to content providers with less confidential information, who nevertheless do not want to disclose it too easily to portals.

Secure Content Embedding

In order to secure the method of "Basic Content Merging" it is preferred that the employs more secure technology like a certificate (x.509) which was issued by a trusted party (like VeriSign) or the vendor, www.medrec.com, itself. The certificate of the user "User1772" is known by Medrec. This can be done when the user signs up.

When the applet sends its request, this is done over an SSLv3/TLS connection. This is one example of a secure connection used in e-commerce. The content provider asks for client certification and Susan's browser proves to the server that it is a valid owner of the certificate (e.g. that it has the private key). Thus, www.medrec.com can make sure that:

- the request is coming on behalf of User1772, e.g. Susan.
- the data is transmitted in a secure fashion via SSL/TLS.

Furthermore, www.medrec.com can require that the applet is loaded in a secure connection. This will prevent anyone from faking or tampering with the Java applet which is running on Susan's browser.

Note that the cookie validation as described above can be used together with the certificate. Security would be enhanced in such a way that certificate theft can only be exploited for a number of days.

Secure Content Embedding with Licensing

The last addition to content merging introduces a method which allows the content provider to license the use of content merging to portals. This is important to verify that content is only merged to pages which are authorized by the content provider. This can be important in order to enforce and protect commercial agreements (exclusive rights, etc.).

The Java applet carries a list of licensed portal sites. When it is transferred and started on Susan's browser it finds the URL of the document where it should place the content. This would be "www.portal.com" herein. It then checks to see if this URL is in its list of licensees. If the URL is not listed it aborts execution with an error message.

A sequence diagram for Content Embedding with Licensing is given in Figure 2.

Implementation Details

The code in the portal's HTML page will contain the following fragment:

```
<div id="medrec" name="medrec">
        <APPLET code="Portal.class" height=0 name="Applet"
        codebase="https://www.medrec.com/"
        width=0 VIEWASTEXT MAYSCRIPT id=Applet>
        <PARAM NAME="foreground" VALUE="FFFFFF">
        <PARAM NAME="background" VALUE="008000">
        </APPLET>

        All this will be replaced.<br>
</div>
```

For browsers which support DHTML, the following Javascript function is added to the page:

```
<script language="javascript">
        function replace() {
         var app = document.applets["Applet"];
         feld.innerHTML = app.getHTML();
        }
</script>
```

For browsers without DHTML, the following function is added to the page:

```
<script language="javascript">
        applet = document.applets["Applet2"];
        s = applet.getHTML();
        document.writeln(s);
</script>
```

The applet initiates the connection to www.medrec.com when the method "getHTML" is called. It returns the HTML fragment in a string, which is then made part of the document from the portal.

As for the licensing method, the applet can use the method "getDocumentBase" of the standard java applet class . This method returns the URL of the document, which can be used for confirmation of the license status.

What is claimed is:

1. A method for creating secure access to data in a first secure file by way of an insecure portal in a distributed computing environment, the process comprising:

accessing an insecure portal provider by a requestor using a browser,

creating, by the requestor, a document unique to the requestor on that insecure portal,

embedding, by said portal in said document, a reference to a java applet which can open a connection to the first secure file,

causing the requestor's browser, while loading the insecure document, to see the java applet and request it from the secure file,

transferring the requested java applet to the requestor's browser which starts it, thereby opening a connection to the secure file,

causing the secure file to generate code which is transmitted to the requestor's browser,

causing the applet on the requestor's browser to receive said code and insert it into the portal's document.

2. A means for accessing a secure file through an insecure portal on a distributed computing system, the process comprising:

activating a java applet embedded in the insecure portal document wherein the java applet which provides secure access to the secure file, wherein the embedded applet is created by:

accessing an insecure portal provider by a requestor using a browser,

creating, by the requestor, a document unique to the requestor on that insecure portal,

embedding, by said portal in said document, a reference to a java applet which can open a connection to the first secure file,

causing the requestor's browser, while loading the insecure document, to see the java applet and request it from the secure file,

transferring the requested java applet to the requestor's browser which starts it, thereby opening a connection to the secure file,

causing the secure file to generate code which is transmitted to the requestor's browser,

causing the applet on the requestor's browser to receive said code and insert it into the portal's document.

3. A means for providing secure access via the internet to a secure file via an insecure portal, as described herein.

Figure 1

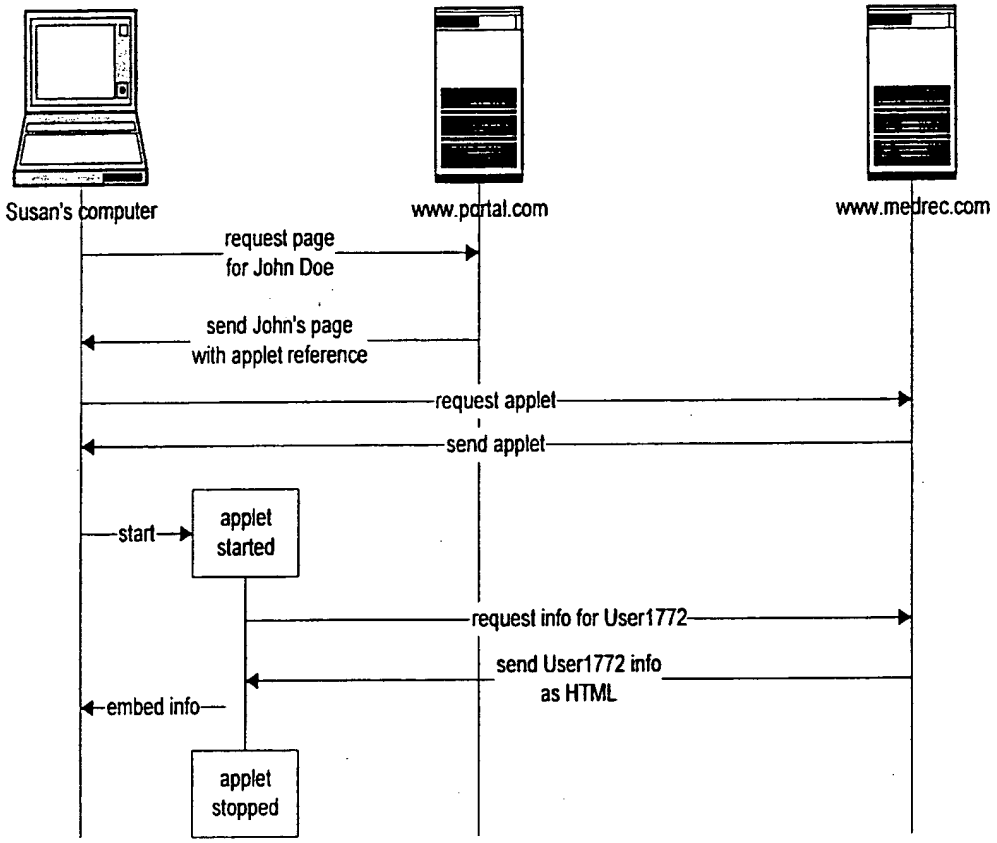
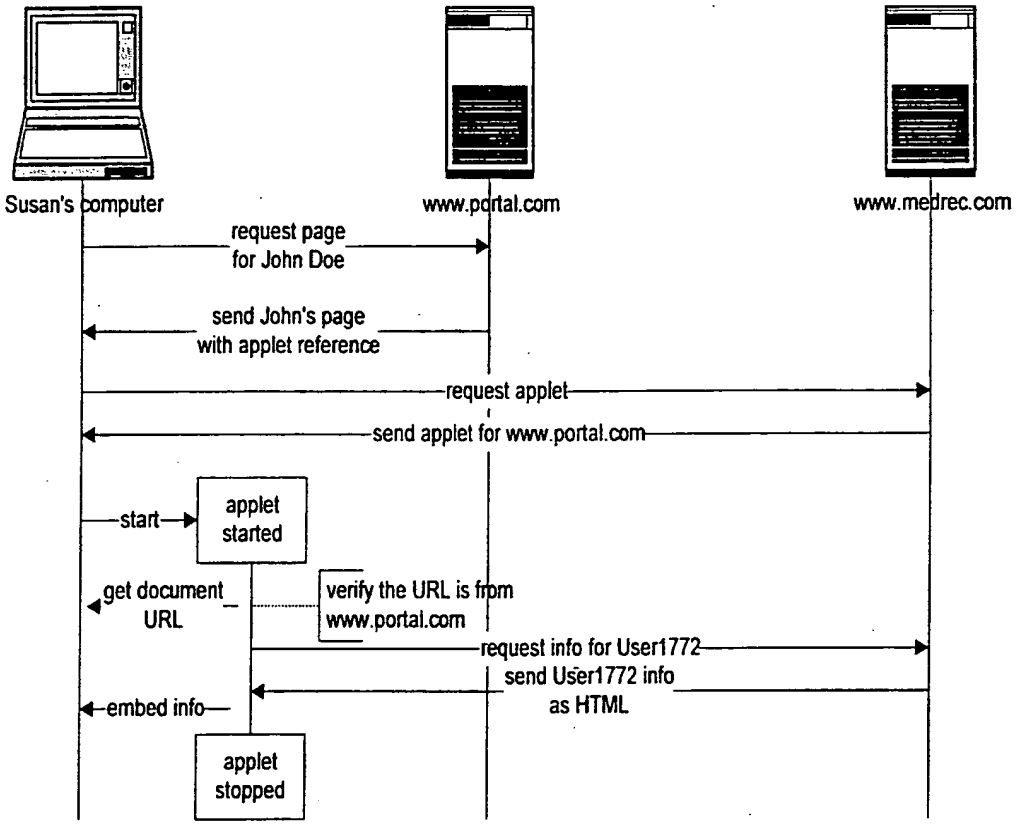

Susan's computer
www.portal.com
www.medrec.com
request page for John Doe
send John's page with applet reference
request applet
send applet
start
applet started
request info for User1772
send User1772 info as HTML
embed info
applet stopped

Figure 2


Susan's computer
www.portal.com
www.medrec.com
request page for John Doe
send John's page with applet reference
request applet
send applet for www.portal.com
start
applet started
get document URL
verify the URL is from www.portal.com
request info for User1772
send User1772 info as HTML
embed info
applet stopped